

Re: [Full-disclosure] Inside AV engines?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-12/msg00113.html>

- *From:* "ad@xxxxxxxxxxxxxxxxxxxx" <ad@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 13 Dec 2005 00:17:07 +0100
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

I would like to have much time to explain you clearly how to but sorry I will do quick cos I disconnect soon:

what do you need to do on the infected file is to split it in different part with the same size, then you sort out the infected part and the one not. you re-split those files again but in smaller size, you sort out again the infected one and the one not , etc , you will find out quickly the detected signature with a byte precision.

tip: a tool outta there does it really well , its name UKSpliter, its place, google :)

nb: this method is useless when the av detects a MD5 checksum as pestpatrol, you change any byte and this is no more detected then...

This is the ultimate way to trick all antivirus , in the old days , had made the famous rootkit hackerdefender undetected by all of them, to note sophos and kav harder to trick because they detects signatures , wich modded, will probably break your proggie..

cheers to undergroundkonnekt guys :)

Jeroen wrote:

- > For penetration testing on Wintel system, I often use netcat.exe and stuff
- > like pwdump. More and more I need to disable anti-virus services before
- > running the tools to avoid alarms and auto-deletion of the applications. It
- > works but it isn't an ideal situation since theoretically a network can be
- > infected while the AV-services are down. Recompiling tools is an option
- > since the source of many tools I use is available. The question is (before I
- > burn useless CPU cycles): can someone help me getting info about the inside
- > of AV engines? Will addition of some rubbish to the code do the trick (->
- > other checksum), do I need to change some core code or is it a mission
- > impossible anyway? Who can help for example getting some useful research
- > papers on the subject of detecting viruses and how to bypass mechanisms
- > used? Any help will be appreciated.
- >

Re: [Full-disclosure] Inside AV engines?

>
> Greetings,
>
> Jeroen
>
>
>
> _____
> Full-Disclosure – We believe in it.
> Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
> Hosted and sponsored by Secunia – <http://secunia.com/>
>
>
>

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.2 (MingW32)

iQIVAwUBQ54E86+LRXunpxfAQLAww//Zush1/OE+akYbRfK8DS5l+QVSmQxcAMu
+itH0H5uNAR83/EWmzVxSK75j6qKqs7EiqL8TcDhXfEU6hwBN+IXz827kaa/ZOhX
N5yE17fSxTWuWI7G7MkHmiZv9gdk2M0ior+uf8HCXGZ4s+giDJNffsoBBSKtE6x+
7kreEuDS2g6jyx7Qv0phoX/GrlTClrCEzcApOO10sq6ItD0HQGF3c+2OuIQkQz
WS4A7TIwj6/XUipS7uy32chUaoFNdf0sgMAP2Vbj1LCIOk2pWfwHG33JrCHb0cg+
so6oYxHZpkN1Lsnr5mDgDZ55589VHihv194Y8EDTt03J6E7OQ2qJX5uwdKB/8iVs
086Ak+1uXYf8PKD6SnAdurOfP9eQpUD7zIs8bXDE74vmjJt5oc++W5RMf+a40+Cj
RukAi2OME39bi3jLaNg/r5g6D0sKQ9uhx45S3h5ziyPGswK6iFQoTfnyb3gRyhs9
5f7CWKjaEihI4qn1R+WkYq7wpsPjnufCtjOZfvuFhi2bFiwnPkbkrTckle4+QGXF
dVrv8ki5sYxC3qgPcKGOjgKXeQ2vLA6vrxpRo/lMJp3RqGv4nEpQXCza2jx8scrs
2IkjJskzmC8sBaSCJ6xgMeQjAjql8lVClIbPmAQYOaX8owLZ9IZsqiPE/g+sFDu+
h1d0xyOwpH4=
=xowQ
-----END PGP SIGNATURE-----

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do! Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831

- **References:**
 - ◆ **Inside AV engines?**
 - ◇ From: Jeroen

Re: [Full-disclosure] Inside AV engines?

Re: [Full-disclosure] Inside AV engines?

- Prev by Date: *Inside AV engines?*
- Next by Date: *Re: [Full-disclosure] Inside AV engines?*
- Previous by thread: *Inside AV engines?*
- Next by thread: *Re: [Full-disclosure] Inside AV engines?*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*